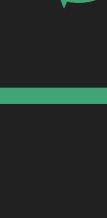


# FortiGuard Labs Outbreak Alerts



## F5 BIG-IP & BIG-IQ Vulnerabilities

### Critical Bug Allowing Remote Code Execution

[https://www.f5.com/services/support/March2021\\_Vulnerabilities](https://www.f5.com/services/support/March2021_Vulnerabilities)

CVEs: CVE-2021-22986, CVE-2021-22987, CVE-2021-22991, CVE-2021-22992

The 2 most critical vulnerabilities allow a remote attacker with access to the user interface (or REST API via the user interface) to gain full control of the system and execute arbitrary system commands, create or delete files, and disable services. The most critical is unauthenticated. Exploitation can lead to complete system compromise. The U.S. Cybersecurity and Infrastructure Agency (CISA) has urged companies using BIG-IP and BIG-IQ to fix the critical F5 flaws.

#### Background

These are 'in the wild' vulnerabilities for existing software - refer to versions listed by F5 to see if you are impacted based on the versions you may be running. Details for the 2 most critical vulnerabilities can be found in the big tables on these articles:-

<https://support.f5.com/csp/article/K18132488>

<https://support.f5.com/csp/article/K03009991>

#### Latest Developments

March 20, 2021: On March 20, multiple stories reported the F5 vulnerabilities under 'active attack'. FortiGuard IPS Threat Signal Report is available from:

<https://www.fortiguard.com/threat-signal-report/3891>

March 10, 2021: F5 announced several vulnerabilities and strongly urged customers to upgrade:

[https://www.f5.com/services/support/March2021\\_Vulnerabilities](https://www.f5.com/services/support/March2021_Vulnerabilities)

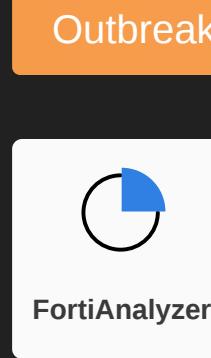


## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

### AV

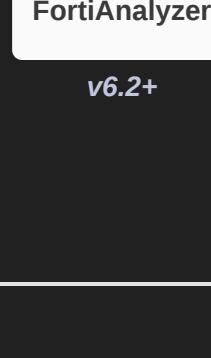
Detects known malware related to the Outbreak



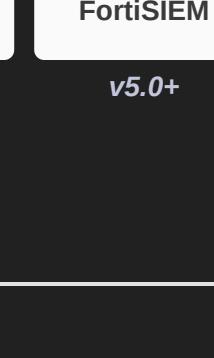
FortiADC

### IPS

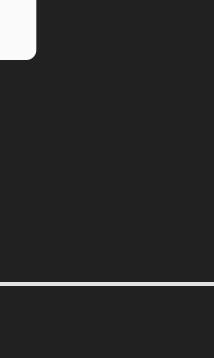
Detects and blocks attack attempts leveraging the vulnerability



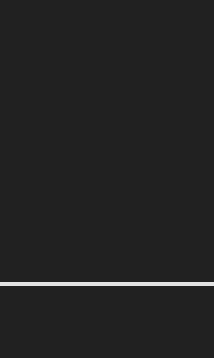
FortiADC



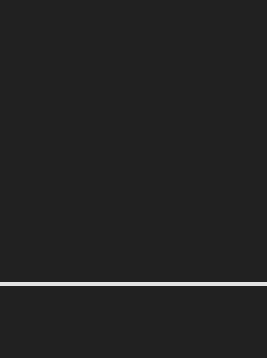
FortiGate



FortiNDR



FortiProxy



FortiSASE

## DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

### IOC



FortiAnalyzer



FortiSOCaaS



FortiSIEM



FortiSOAR

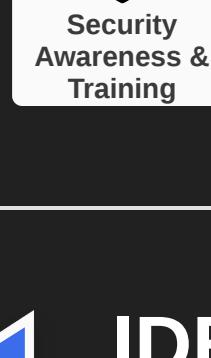
### Outbreak Detection



FortiAnalyzer

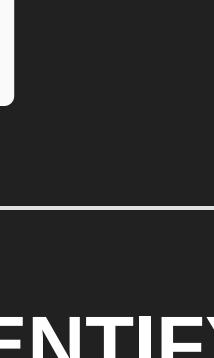
DB 1.00033

### Threat Hunting



FortiAnalyzer

v6.2+



FortiSIEM

v5.0+



## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

### NOC/SOC Training

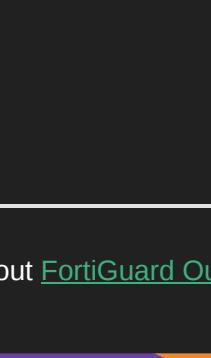


NSE Training



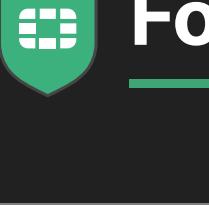
Response

### End-User Training



Security Awareness & Training

Learn more about [FortiGuard Outbreak Alerts](#)



## IDENTIFY

Identify processes and assets that need protection:

### Attack Surface Hardening



Rating

Learn more about [FortiGuard Outbreak Alerts](#)



## FortiGuard Labs